IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Kotaro Kaneko	)	Group Art Unit: 2435
	)	
Application No.: 10/647,383	)	Examiner: April Ying Shan
	)	
Filed: August 26, 2003	)	Confirmation No. 2047
	)	
For: CONTROLLING COMPUTER PROGRAM, CONTROLLING APPARATUS, AND CONTROLLING METHOD FOR DETECTING INFECTION BY COMPUTER VIRUS	)	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal is from the decision of the Examiner in the Final Office Action dated August 17, 2009, and Appellant's Notice of Appeal filed January 12, 2010, setting a period for response that extends through April 12, 2010, by a Petition for Extension of Time (one month) filed herewith.

Please charge the $540.00 fee for filing this Appeal Brief to credit card. The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

I. Real Party in Interest

Minolta Co., Ltd. is the real party in interest, and is the assignee of Application No. 10/647,383.

II. Related Appeals and Interferences

None.

III. Status of Claims

The application contains claims 1-26. Claims 1-4, 11-14, 19 and 24-26 are pending and stand rejected. Claims 5-10, 15-18 and 20-23 are cancelled. This appeal is directed to the rejections of pending claims 1-4, 11-14, 19 and 24-26.

IV. Status of Amendments

No claim amendments were submitted subsequent to the final Office Action dated August 17, 2009.

V. Summary of Claimed Subject Matter

The claimed invention provides a method and computer program for causing a controlling apparatus intended to control an image forming apparatus, as well as a controlling apparatus for controlling an image forming apparatus. An exemplary configuration of the controlling apparatus is illustrated in Figure 1, in which a computer 200 is limited to controlling an image forming apparatus such as copying machine 300 (see paragraph [0023] on page 7 of the specification).

As illustrated in Figure 3, a hard disk 204 of the computer 200 includes a database 240 in which a file list 241 and running program status list 242 are stored. The file list 241 is a list of all files, such as programs, which are required to exist in a specific storage area of a logical drive of hard disk 204 for controlling a multifunctional peripheral (MFP) 100 that includes the computer 200 and copying/scanning machine 300 (see, e.g., paragraph [0039]). The running program status list 242 is a list of all programs running on the MFP 100 for controlling the MFP 100. As described in paragraph [0041] on page 11, the file list 241 and running program status list 232 are set up prior to factory shipment of MFP 100 and the controlling apparatus, and are stored in the hard disk 204 of the controlling apparatus. Accordingly, the file list 241 is a preset list of programs and files that are authorized to be run on the controlling apparatus to control the image forming apparatus, such as the copying/scanning machine 300 illustrated in Figure 1, for example.

According to the exemplary configuration in which the controlling apparatus (e.g., computer 200) is limited to controlling an image forming apparatus, the controlling apparatus is different from a general-purpose computing device in which a user may wish to add, modify or remove programs and files at will for various purposes. On the other hand, since the function of the controlling apparatus is limited to controlling the image forming apparatus, according to the exemplary configuration illustrated in Figure 1, the preset list of programs in the file list 241 represents a limited number of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus.

Therefore, the claimed invention provides that programs that are authorized to be run to control the image forming apparatus are included in a preset list 241 of

programs, and the preset list 241 is stored in the controlling apparatus (e.g., computer 200). This preset list 241 therefore contains programs that are known (i.e, approved) to control the image forming apparatus (e.g., copying machine 300). However, if a program is confirmed to be running on the controlling apparatus and that confirmed program is not included in the preset list 241 of programs, the confirmed program is judged to be an illegal program resulting from a computer virus infection.

When a computer virus infiltrates into a computer, the virus often creates a new program and/or file. In the case of a general-purpose computing device, the number of programs and files that can be run is not limited to a preset list, due to the desire to allow users to add new programs or files and modify or delete existing programs or files. For example, general purpose computing devices are configured to allow users to add software programs containing executable and non-executable files, and add new non-executable files, such as a word processing document, for example. Therefore, conventional virus detection systems seek to compare a file against files that are known to be created by known viruses.

On the other hand, since the preset list of programs in the file list 241 represents a limited number of programs that are authorized be run on the controlling apparatus to control the image forming apparatus, the detection of a program that is not included in the file list 241 is judged to be an illegal program resulting from a computer virus infection. This judgment can be carried out because a limited number of programs that are authorized to be run on the controlling apparatus are stored in the preset list of programs.

These features of the claimed invention would be disadvantageous to the functions and purpose of a general-purpose computer. In particular, limiting a general-purpose computer to a preset list of programs would defeat the purpose of permitting a user to create, add and modify files and programs on the general-purpose computer. On the contrary, general-purpose computers are designed to allow dynamic modifications. Consequently, virus detection and prevention systems for general-purpose computers detect programs do <u>not</u> judge a file or program that is <u>not included</u> in a list of authorized programs or files to be an illegal program resulting from a computer virus, because such a system would severely limit the functionality

of a general-purpose computer in allowing its user to create, add and/or modify existing files with the general-purpose computer.

The present application contains three (3) independent claims: claims 1, 11 and 19. A mapping of the independent claims to an exemplary embodiment described in the disclosure is set forth in the following table. Paragraph numbers identified below refer to the original specification.

Claim 1	Supporting Disclosure
A computer program stored on a computer-readable recording medium and causing a controlling apparatus intended to control an image forming apparatus to execute the procedures of:	Examples of computer-readable recording medium include ROM 202 and hard disk 204, which are comprised in computer 200, as illustrated in Fig. 2. See, e.g., ¶ [0026], as well as ¶¶ [0022] and [0023], which describe that the purpose of computer 200 is limited to controlling an image forming apparatus such as copying/scanning machine 300 of multi-function peripheral (MFP) 100 (see ¶ [0025] and Fig. 1). ¶ [0028] provides that a virus scan program 220 (see Fig. 3) is installed on hard disk 204, and ¶ [0029] provides that CPU 201 (see Fig. 2) executes the virus scan program 220. Function modules of the virus scan program 220 are described in ¶ [0033].
storing a preset list of programs that are authorized to be run on said controlling apparatus to control the image forming apparatus;	File list 241 and running program status list 242 are stored in database 240 (see, e.g., ¶¶ [0033], [0039]).
confirming each program running on said controlling apparatus;	Virus scan program 220 comprises a running program status scan module 223 (see, e.g., ¶¶ [0033]

	and [0036], Fig. 3, and step S117 in Fig. 5).
judging a program, which is not included in the preset list of programs that are authorized to be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection; and	Running program status scan module 223 judges a program which is not included in running program status list 242 as an illegal program (see, e.g., ¶ [0036] and [0079]).
deleting or isolating the program that is judged to be an illegal program.	See, e.g., ¶¶ [0035], [0036], [0070], [0071], [0078] and [0079], and steps S116 and S119 in Fig. 5.
Claim 11	**Supporting Disclosure**
A controlling apparatus for controlling an image forming apparatus, said controlling apparatus comprising:	Computer 200 illustrated in Figs. 1 and 2 is an example of a controlling apparatus. See, e.g., paragraph [0022].
a storage unit for storing in advance a preset list of programs that are authorized to be run on said controlling apparatus for controlling said image forming apparatus; and	File list 241 and running program status list 242 are stored in database 240 (see, e.g., ¶¶ [0033], [0039]).
a processor connected to said storage unit, wherein said processor is configured to confirm each program running on said controlling apparatus, and judge a program, which is not included in said preset list of authorized programs among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection.	¶ [0028] provides that a virus scan program 220 (see Fig. 3) is installed on hard disk 204, and ¶ [0029] provides that CPU 201 (see Fig. 2) executes the virus scan program 220. Virus scan program 220 comprises a running program status scan module 223 (see, e.g., ¶¶ [0033] and [0036], Fig. 3, and step S117 in Fig. 5). Running program status scan module 223 judges a program which is not included in running program status list 242 as an illegal program (see,

	e.g., ¶ [0036] and [0079]). ¶¶ [0035], [0036], [0070], [0071], [0078] and [0079], and steps S116 and S119 in Fig. 5, for example, describe that the program confirmed to be running but not in the preset list 241 and/or running program status list 242 are judged as illegal programs.
Claim 19	**Supporting Disclosure**
A controlling method for a controlling apparatus intended to control an image forming apparatus, comprising the steps of:	¶ [0028] provides that a virus scan program 220 (see Fig. 3) is installed on hard disk 204, and ¶ [0029] provides that CPU 201 (see Fig. 2) executes the virus scan program 220. Function modules of the virus scan program 220 are described in ¶ [0033].
storing a preset list of programs that are authorized to be run on said controlling apparatus to control the image forming apparatus	File list 241 and running program status list 242 are stored in database 240 (see, e.g., ¶¶ [0033], [0039]).
confirming each program running on said controlling apparatus;	Virus scan program 220 comprises a running program status scan module 223 (see, e.g., ¶¶ [0033] and [0036], Fig. 3, and step S117 in Fig. 5).
judging a program, which is not included in the preset list of programs that are authorized to be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from computer virus infection; and	Running program status scan module 223 judges a program which is not included in running program status list 242 as an illegal program (see, e.g., ¶ [0036] and [0079]).
deleting or isolating the program that is judged to be the illegal program.	See, e.g., ¶¶ [0035], [0036], [0070], [0071], [0078] and [0079], and

	steps S116 and S119 in Fig. 5.

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action contains a single ground of rejection. The ground of rejection to be reviewed on appeal is whether claims 1-4, 11-14, 19 and 24-26 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent No. 5,918,009 to Togawa et al. (hereinafter "Togawa") in view of Applicant's Admitted Prior Art (hereinafter "AAPA").

VII. Argument

A. Independent Claims 1, 11 and 19

Claim 1 recites a computer program stored on a computer-readable recording medium and causing a controlling apparatus intended to control an image forming apparatus to execute the following procedures:

(1) storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus;

(2) confirming each program running on the controlling apparatus;

(3) judging a program, which is **not included** in the preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection; and

(4) deleting or isolating the program that is judged to be the illegal program.

Claim 11 recites a controlling apparatus for controlling an image forming apparatus. The controlling apparatus of claim 11 comprises a storage unit for storing in advance a preset list of programs that are authorized to be run for controlling the image forming apparatus. The controlling apparatus of claim 11 also comprises a processor that is configured to perform functions corresponding to procedures (2)-(3) of claim 1. Claim 19 recites a controlling method for a controlling apparatus intended to control an image forming apparatus. The method of claim 19 comprises steps corresponding to procedures (1)-(4) of claim 1.

Accordingly, features (1)-(3) of claim 1 are common to each of independent claims 1, 11 and 19. Claims 1, 11 and 19 thus each recite that a preset list of programs is stored. The preset list of programs are authorized to be run on the controlling apparatus to control the image forming apparatus. In addition, claims 1, 11 and 19 each recite that each program running on the controlling apparatus is confirmed, and a program, which is **not included** in the preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, is judged as an illegal program resulting from a computer virus infection.

The Examiner alleges that Togawa discloses all the features of claims 1, 11 and 19, except for the feature of a controlling apparatus that controls an image forming apparatus. The Examiner alleges that the AAPA cures the deficiencies of Togawa for failing to disclose or suggest this feature. The rejections of claims 1, 11 and 19 are legally and factually erroneous, for at least the following reasons.

Togawa discloses a storage device that prevents files stored thereon from being infected with a computer virus. The function of the storage device of Togawa is to have the ability to freely use files stored thereon with a personal computer while preventing the breeding of a virus and to delete a file infected with a virus or restore the infected file into an uninfected state (see Column 1, lines 25-28). With reference to Figure 2, the storage device 1 includes a disk 10 on which files are stored, and a virus checker 15. The virus checker 15 can be activated at periodic intervals or on command (see Column 8, lines 18-21). The storage device 1 also includes a table registering means 17 which registers a virus-infected file that is detected by the virus checker 15 in a infection management table means 16 (see Column 8, lines 21-28 and 58). The infection file management table means 16 functions as a repository for virus-infected files, and the table registering means 17 writes the virus-infected files into the infection management table means 16.

When a request for access to one of the files stored on the disk 10 is received, a judging means 18 references the infection file management table means 16 to determine if the requested file is infected with a virus. That is, the judging means 18 references the infection file management table means 16 to determine if the requested file has been registered as a virus-infected file in the infection file

management table means 16, in which case it is judged that the requested file is infected with a virus (see Column 8, lines 25-29).

Figure 3 of Togawa illustrates an implementation of the storage device 1 being connected to a personal computer 2a, i.e., a general-purpose computer (see Column 10, lines 11-13). As illustrated in Figure 3, the storage device 1 includes an original information management file 34, which is used to manage original information of files stored in the disk 30, and original information of a virus checker prepared for inspecting the files stored on the disk 30 (see Column 10, lines 23-27). The storage device 1 also includes a version upgrade information management file 35, which is used to manage differential information (i.e., version update information) concerning a file stored in the disk 30, and history information (i.e., version update history information) concerning the differential information brought about due to modification. In addition, the version information management file 35 is used to manage differential information concerning an upgraded version of the virus checker (i.e., virus definition update information), and history information concerning the history of modifications of the information of the virus checker (i.e., virus definition update history information) (see Column 10, lines 34-35).

In the final Office Action dated August 17, 2009, the Examiner alleged that the original information management file 34 of Togawa corresponds to the preset list of programs as recited in claims 1, 11 and 19, and that the differential information contained in the version information management file 35 of Togawa corresponds to a program which is not included in the preset list of programs as recited in claims 1, 11 and 19.

The Examiner's assertion that Togawa discloses the judging operation of claims 1, 11 and 19 is contrary to the *actual* disclosure of Togawa. In particular, the system of Togawa requires a priori knowledge of whether a file or program constitutes a virus, or else the virus checker would not be capable of detecting if a file stored on the disk 30 is infected with the virus. This is evidenced by the need for original information of the virus checker, as well as the differential information of the virus checker, which is virus definition version update information.

Togawa does not disclose or suggest that a file which is **not included** in the original information management file 34 is judged to be a file having been infected with a virus. On the contrary, Togawa discloses an entirely different configuration, in

which the virus checker determines whether files that **are included** in the original information management file 34 and/or the differential information that **is included** in the version information management file 35 are infected with a virus, with reference to the original information of the virus checker and any updated virus definition information (differential information) of the virus checker (see Column 10, lines 35-41 and Column 13, lines 28-36).

The Examiner alleged that because the original information stored in the original information management file 34 can be updated and stored as differential information in the version information management file 35, that this updating operation somehow corresponds to judging whether a file which is **not included** in a preset list of authorized programs is judged to be an illegal program. This interpretation is not supportable. The virus checker of Togawa does not determine that a file which **is included** in the original information management file 34 has been infected with a virus if there is corresponding difference information in the version information management file 35.

Furthermore, in either case of whether the virus checker determines whether files which **are included** in the original information management file 34 or differential information which **is included** in the version information management file 35 have been infected with a virus, the virus checker determines whether files and/or information which **are included** in a file 34, 35 have been infected with a virus.

Moreover, it is unclear how updating original information is related in any way to judging that a file which is **not included** in a preset list of authorized programs is an illegal file. On the contrary, the fact that the original information stored in the original information management file 34 can be updated contradicts the Examiner's unsupportable interpretation of Togawa. For the original information to be updated, it must therefore have already been stored. Information cannot be updated unless it has been stored previously. Therefore, the virus checking operation of Togawa and the subsequent quarantining of infected files involves a judgment of files **which are included** in the disk 30 and therefore **are included** in the original information management file 34.

The Examiner disregarded a fundamental distinction between Togawa and the claimed invention, in that Togawa discloses that files and/or information which **are included** in the files 34, 35 are checked for viruses. Accordingly, the virus

checking operation of Togawa and the subsequent quarantining of infected files involves a judgment of files **which are included** in the disk 30 and therefore **are included** in either the original information management file 34 and/or the version information management file 35. Therefore, the virus checker of Togawa determines whether known files stored on the disk 30 are infected with a virus.

It appears that the Examiner has not fully appreciated a fundamental distinction between the claimed invention and systems such as Togawa which are for use with general-purpose computers. Claims 1, 11 and 19 recite that a program which is **not included** in the preset list of programs is judged to be an illegal program resulting from a computer virus infection. On the other hand, Togawa discloses that files which **are included** in the original information management file 34 are checked for viruses.

Therefore, Appellant respectfully submits that Togawa does not disclose, suggest or contemplate that files which are **not included** in the original information management file 34 are judged to be illegal files resulting from a computer virus infection. On the contrary, Togawa discloses the opposite configuration.

Accordingly, for at least the foregoing reasons, Appellant respectfully submits that Togawa does not disclose or suggest:

(1) storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus; and

(3) judging a program, which is **not included** in a preset list of programs that are authorized be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection, as recited in claims 1, 11 and 19.

Furthermore, Togawa does not disclose or suggest that the original information management file 34 stores files to control the controller 38. On the contrary, Togawa merely discloses that the files identified in the original information management table 34 represent the files that are stored on the disk 30. The controller 38 accesses files stored on the disk 30, original information managed in the original information management file 34, and accesses the differential information (version update information of the files and virus definition version update information of the virus checker) in the version upgrade information management file 35 (see Column 10, line 66 to Column 11, line 5).

It is unclear how the Examiner reached the unsupported interpretation that the original information stored in the original information management file 34 somehow controls the controller 38. Furthermore, Togawa does not disclose or suggest that the original information stored in the original information management file 34 has been authorized to be run by the controller 38. The storage device 1 of Togawa is, as mentioned above, for use with a general-purpose computer (e.g., personal computer 2a). Therefore, it is antithetical and disadvantageous for the function of the personal computer 2a to have limited uses and functions by having a limited number of files and/or programs stored in the original information management file 34 for supposedly controlling the controller 38.

Furthermore, Appellant respectfully submits one skilled in the art would not have reason or been motivated to modify Togawa to arrive at the subject matter of claims 1, 11 and 19. The technique of Togawa is disclosed for general purpose computing devices, not for a controlling apparatus intended to control an image forming apparatus in which the programs that are authorized to be run therefor are included in a preset list of programs.

Similar to Togawa, AAPA also does not disclose or suggest storing a preset list of programs that are authorized to be run to control an image information apparatus, and judging a program which is **not included** in the preset list of programs as an illegal program resulting from a computer virus infection, as recited in claims 1, 11 and 19.

Consequently, AAPA does not cure the deficiencies of Togawa for failing to disclose or suggest all the recited features of claims 1, 11 and 19.

Therefore, no obvious combination of Togawa and AAPA can result in the subject matter of claims 1, 11 and 19, since Togawa and AAPA, either individually or in combination, fail to disclose or suggest all the recited features of claims 1, 11 and 19.

Accordingly, for at least the foregoing reasons, Appellant respectfully submits that claims 1, 11 and 19, as well as claims 2-4, 12-14 and 24-26 which depend therefrom, are patentable over Togawa and AAPA.

B. Dependent Claims

Dependent claims 2-4, 12-14 and 24-26 recite further distinguishing features over Togawa and the AAPA.

For instance, claims 2, 12 and 24 recite that a program which is judged to be an illegal program is automatically deleted or isolated in response to judging that the program is an illegal program. The Examiner alleges that this feature of claims 2, 12 and 24 is disclosed in step S211 in Fig. 21 of Togawa. Appellant respectfully disagrees.

Fig. 21 of Togawa illustrates an operation that occurs when an operator of the general-purpose computer 2a inputs a command instructing restoration of a virus-infected file that is stored on the hard disk 30 (see Column 18, lines 48-57). Accordingly, step S211 in Fig. 21 of Togawa does not involve an operation of automatically deleting or isolating a program which is judged to be an illegal program.

Claims 3, 13 and 25 recite that the feature of judging a program which is not included in a preset list of programs that are authorized to be run on the controlling apparatus includes comparing the name of each program whose running state has been confirmed with the name of each program included in the preset list. Togawa cannot disclose or suggest this feature. As discussed above, Togawa does not disclose, suggest or contemplate the feature of storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus. Such a feature would be antithetical to the features of a general-purpose computer, due to the desire to allow users to create, modify and add files and/or programs. Accordingly, since Togawa does not in any way disclose or suggest storing a preset list of programs that are authorized to be run on the general purpose computer 2a, Togawa cannot disclose or suggest the feature of comparing the name of each program whose running state has been confirmed with the name of each program included in the preset list, to judge whether the program is an illegal program, as recited in claims 3, 13 and 25.

Claims 4, 14 and 25 recite that the feature of judging a program which is not included in a preset list of programs that are authorized to be run on the controlling apparatus includes comparing the size of each program whose running state has been confirmed with the size of each program included in the preset list. Togawa

cannot disclose or suggest this feature. As discussed above, Togawa does not disclose, suggest or contemplate the feature of storing a preset list of programs that are authorized to be run on the controlling apparatus to control the image forming apparatus. Such a feature would be antithetical to the features of a general-purpose computer, due to the desire to allow users to create, modify and add files and/or programs. Accordingly, since Togawa does not disclose or suggest storing a preset list of programs that are authorized to be run on the general purpose computer 2a, Togawa cannot disclose or suggest the feature of the comparing the size of each program whose running state has been confirmed with the size of each program included in the preset list, to judge whether the program is an illegal program, as recited in claims 4, 14 and 26.

Accordingly, for at least the foregoing reasons, Appellant respectfully submits that dependent claims 2-4, 12-14 and 24-26 recite further distinguishing features over Togawa and the AAPA.

C. Conclusion

Appellant has pointed to errors in the rejections of the claims including mischaracterizations and misinterpretations of the applied art, in addition to the failure of the applied art in disclosing or suggesting all the recited features of the claimed invention. Therefore, Appellant respectfully requests that the final rejection be overturned and the application be returned to the Examiner for prompt allowance.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

None.

X. Related Proceedings Appendix

None.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date April 12, 2010

By: /Jonathan R. Bowser/
Jonathan R. Bowser
Registration No. 54574

Customer No. 21839
703 836 6620

VIII. CLAIMS APPENDIX

The Appealed Claims

Claims involved in the appeal of U.S. Patent Application Serial No. 10/647,383:

1. A computer program stored on a computer-readable recording medium and causing a controlling apparatus intended to control an image forming apparatus to execute the procedures of:

storing a preset list of programs that are authorized to be run on said controlling apparatus to control the image forming apparatus;

confirming each program running on said controlling apparatus;

judging a program, which is not included in the preset list of programs that are authorized to be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection; and

deleting or isolating the program that is judged to be an illegal program.

2. A computer program of claim 1, wherein the procedure of deleting or isolating the illegal program includes automatically deleting or isolating the illegal program in response to said judgment.

3. A computer program of claim 1, wherein the procedure of judging includes a procedure of comparing the name of each program whose running state has been confirmed with the name of each program included in said preset list.

4. A computer program of claim 1, wherein the procedure of judging includes a procedure of comparing the size of each program whose running state has been confirmed with the size of each program included in said preset list.

11. A controlling apparatus for controlling an image forming apparatus, said controlling apparatus comprising:

a storage unit for storing in advance a preset list of programs that are authorized to be run on said controlling apparatus for controlling said image forming apparatus; and

a processor connected to said storage unit, wherein said processor is configured to confirm each program running on said controlling apparatus, and judge a program, which is not included in said preset list of authorized programs among programs whose running states have been confirmed, as an illegal program resulting from a computer virus infection.

12. A controlling apparatus of claim 11, wherein said processor is configured to automatically delete or isolate the program that is judged to be the illegal program.

13. A controlling apparatus of claim 11, wherein said processor is configured to compare the name of each program whose running state has been confirmed with the name of each program included in said preset list.

14. A controlling apparatus of claim 11, wherein said processor is configured to compare the size of each program whose running state has been

confirmed with the size of each program included in said preset list.

19. A controlling method for a controlling apparatus intended to control an image forming apparatus, comprising the steps of:

storing a preset list of programs that are authorized to be run on said controlling apparatus to control the image forming apparatus;

confirming each program running on said controlling apparatus;

judging a program, which is not included in the preset list of programs that are authorized to be run to control the image forming apparatus among programs whose running states have been confirmed, as an illegal program resulting from computer virus infection; and

deleting or isolating the program that is judged to be the illegal program.

24. A controlling method of claim 19, wherein the step of deleting or isolating the illegal program includes automatically deleting or isolating the illegal program in response to said judgment.

25. A controlling method of claim 19, wherein the step of judging includes comparing the name of each program whose running state has been confirmed with the name of each program included in said preset list.

26. A controlling method of claim 19, wherein the step of judging includes

comparing the size of each program whose running state has been confirmed with the size of each program included in said preset list.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None